## AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of managing a communication with a mobile device over a network, comprising:

receiving a request from the mobile device, wherein the request includes associated information;

automatically determining at least one level of trust from a plurality of different levels of trust based, in part, on the associated information, and based on:

if a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device;

if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device; and

if the mobile device is enabled to interact with a Uniform Resource Locator (URL), then determining at least a third level of trust associated with the mobile device; and

determining at least one device signature for the mobile device based on the at least one level of trust from the plurality of different levels of trust, and independent of user authentication.

2. (Original) The method of Claim 1, further comprising:

receiving gateway information, wherein the gateway information is associated with a carrier gateway for the mobile device; and

determining the at least one level of trust based, in part, on the associated information and the gateway information.

3. (Original) The method of Claim 1, wherein the associated information comprises at least one of a device identifier, user agent information, and an indication that the mobile device is enabled to accept a cookie.

4. (Original) The method of Claim 3, wherein the associated information further comprises at least one of a gateway group identifier, and a subscription identifier.

5. (Currently Amended) The method of Claim 1, wherein the method further comprises:

automatically determining a second device signature based on the second level of trust, wherein the second device signature comprises a hash of at least a cookie, a gateway group identifier and a user agent identifier obtainable from the associated information, ~~a second level of trust from the plurality of different levels of trust based, in part, on the associated information; and~~

~~determining a second device signature for the mobile device based on the second level of trust, and independent of user authentication.~~

6. (Original) The method of Claim 1, wherein the associated information further comprises a subscription identifier associated with the mobile device that is based on at least one of a Mobile Identification Number, an Electronic Serial Number, and an application serial number.

7. (Currently Amended) The method of Claim 1, wherein ~~determining the at least one level of trust further comprises:~~ if a trusted mobile device identifier associated with the mobile device is received, further comprises:

determining a level of trust of a carrier associated with the mobile device based on at least one of a received subscription identifier and a gateway group identifier in the associated information; and

if the determined level of trust for the carrier is above a determined level, trusting the received mobile device identifier; and

if the mobile device identifier is trusted, then enabling the determination of at least the first level of trust associated with the mobile device; and

if the mobile device identifier is untrusted, then inhibiting the determination of the at least first level of trust associated with the mobile device.

~~if the associated information comprises a device identifier and trustworthy gateway information, determining a first level of trust.~~

8. (Currently Amended) The method of Claim 1, ~~wherein determining the at least one level of trust further comprises:~~ further comprising:

determining a default level of trust as the third level of trust.

~~if the associated information indicates the mobile device is enabled to accept a cookie, determining a second level of trust.~~

9. (Currently Amended) The method of Claim 1, wherein ~~determining the at least one level of trust further comprises:~~

the mobile device identifier is at least one of a mobile identification number (MIN), an Electronic Serial Number (ESN), application serial number, or a mobile telephone number.

~~if the associated information indicates the mobile device is enabled to use a URL, determining a third level of trust.~~

10. (Currently Amended) The method of Claim 1, wherein determining at least one device signature further comprises:

if [[a]]the first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp.

11. (Currently Amended) The method of Claim 1, wherein determining at least one device signature further comprises:

if [[a]]the second level of trust is determined, determining a second tier device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp.

12. (Currently Amended) The method of Claim 1, wherein determining at least one device signature further comprises:

if [[a]]the third level of trust is determined, determining a third tier device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp.

13. (Original) The method of Claim 12, wherein determining the third tier device signature further comprises including the third tier device signature in a munged URL.

14. (Original) The method of Claim 1, wherein determining at least one device signature further comprises employing a hash function selected from at least one of a Message Digest, a Secure Hash Algorithm (SHA), Digital Encryption Standard (DES), triple-DES, Hash of Variable Length (HAVAL), RIPEMD, and Tiger hash function.

15. (Original) The method of Claim 1, further comprising expiring the at least one device signature based, in part, on a predetermined period of time associated with each of the at least one device signature.

16. (Original) The method of Claim 1, further comprising:

if the at least one device signature has expired, determining if the expired device signature is to be rolled over, and

if the expired device signature is to be rolled over, extending a validity period associated with the expired device signature.

17. (Original) The method of claim 16, wherein determining if the expired device signature is to be rolled over further comprises evaluating at least one of a condition, event, change in an identifier indicating a grouping of the gateway, and a time.

18. (Currently Amended) A client adapted for a mobile device to communicate with a server over a network, the client being configured to perform actions, comprising:

sending a request to the server for content, wherein the request includes an identifier associated with a user agent; and

receiving at least one device signature associated with the mobile device, wherein the at least one device signature is based on at least one level of trust determined from a plurality of different trust levels, and is independent of user authentication, the at least one level of trust being determined based on:

determining at least a default level of trust;

if a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device;

if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device; and

if the mobile device is enabled to interact with a Uniform Resource Locator (URL), then determining at least a third level of trust associated with the mobile device .

19. (Currently Amended) The client of Claim 18, wherein the client is configured to perform actions, further comprising:

providing [[a]]the mobile device identifier based on at least one of a Mobile Identification Number, an Electronic Serial Number, and an application serial number.

20. (Currently Amended) The client of Claim 18, wherein receiving the at least one device signature further comprises:

if the at least one device signature is based on [[a]]the first level of trust, receiving a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, the user agent identifier, and a time stamp.

21. (Currently Amended) The client of Claim 18, wherein receiving the at least one device signature further comprises:

if the at least one device signature is based on [[a]]the second level of trust, receiving a second tier device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, the user agent identifier, and a time stamp.

22. (Currently Amended) The client of Claim 18, wherein receiving the at least one device signature further comprises:

if the at least one device signature is based on [[a]]the third level of trust, receiving a third tier device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp.

23. (Original) The client of Claim 18, wherein sending the request further comprises sending the request to a carrier gateway, wherein the carrier gateway is configured to perform actions, comprising:

modifying the request to include at least one of a subscription identifier associated with the mobile device, and a gateway identifier;

forwarding the modified request to the server;

receiving the at least one device signature from the server; and

forwarding the at least one device signature to the mobile device.

24. (Original) The client of Claim 18, wherein receiving the at least one device signature further comprises, if the request indicates the mobile device is enabled to accept a cookie, associating the cookie with the at least one device signature.

25. (Original) The client of Claim 18, wherein receiving the at least one device signature further comprises, associating a munged Uniform Resource Locator (URL) with the at least one device signature.

26. (Currently Amended) A server for managing a communication with a mobile device over a network, comprising:

a transceiver for receiving a request from the mobile device and for sending at least one device signature to the mobile device; and

a transcoder that is configured to perform actions, including:

receiving the request from the mobile device, wherein the request includes associated information;

automatically determining at least one level of trust from a plurality of different trust levels based, in part, on the associated information and further based on:

if a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device;

if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device; and

if the mobile device is enabled to interact with a Uniform Resource Locator (URL), then determining at least a third level of trust associated with the mobile device; and

determining the at least one device signature for the mobile device based on the at least one level of trust of the plurality of different trust levels, wherein the at least one device signature is independent of user authentication.

27. (Original) The server of Claim 26, wherein the transcoder is configured to perform further action, comprising:

receiving gateway information, wherein the gateway information is associated with a carrier gateway for the mobile device; and

determining the at least one level of trust based, in part, on the associated information and the gateway information.

28. (Currently Amended) The server of Claim 26, wherein determining the at least one device signature further comprises:

if [[a]]the first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp.

29. (Currently Amended) The server of Claim 26, wherein determining the at least one device signature further comprises:

if [[a]]the second level of trust is determined, determining a second tier device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp.

30. (Currently Amended) The server of Claim 26, wherein determining the at least one device signature further comprises:

if [[a]]the third level of trust is determined, determining a third tier device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp.

31. (Currently Amended) The server of Claim 26, wherein determining the at least one level of trust further comprises determining [[a]]the first level of trust based at least one of a

gateway group identifier, a subscription identifier, a user agent, and a security level associated with the request from the mobile device to determine if the mobile device identifier is trusted.

32. (Currently Amended) The server of Claim 26, wherein determining the at least one level of trust further comprises determining [[a]]the second level of trust based at least one of a gateway identifier, and a user agent~~, and whether the mobile device is enabled to accept a cookie,~~.

33. (Currently Amended) The server of claim 26, wherein if a trusted mobile device identifier associated with the mobile device is received further comprises determining that the mobile device identifier is trusted if a carrier gateway associated with the mobile device is trusted. ~~determining the at least one level of trust further comprises determining a third level of trust if the mobile device is enabled to interact with a URL.~~

34. (Original) The server of claim 26, wherein the transcoder is configured to perform further actions, comprising:

determining if at least one device signature has expired device, and

if the expired device signature is to be rolled over, extending a validity period associated with the expired device signature.

35. (Currently Amended) A system for managing a communication with a mobile device over a network comprising:

the mobile device configured to provide information associated with the mobile device; and

a server, coupled to the carrier gateway, that is configured to receive the associated information and to perform actions, including:

automatically determining at least two different levels of trust from a plurality of different levels of trust based, in part, on the associated information, wherein the at least two different levels of trust are based on:

if a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device; and

determining if the mobile device is enabled with a defined operational capability and if the mobile device is so enabled, then determining another level of trust associated with the mobile device; and

initially determining at least two different device signatures for the mobile device each of the two devices signatures being based on a different one of the at least two different levels of trust, wherein the at least two device signatures are each determined independent of user authentication.

36. (Previously presented) The system of Claim 35, wherein determining the at least two device signatures further comprises determining a tier 1 device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp.

37. (Previously presented) The system of Claim 35, wherein determining the at least two device signatures further comprises determining a tier 2 device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp.

38. (Previously presented) The system of Claim 35, wherein determining the at least two device signatures further comprises determining a tier 3 device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp.

39. (Original) The system of Claim 38, wherein the tier 3 device signature is provided to the mobile device through a munged URL.

40. (Original) The system of Claim 35, further comprising:

a carrier gateway, coupled to the mobile device, that is configured to receive the associated information, and provide the associated information and gateway information related to the carrier gateway.

41. (Currently Amended) A computer readable storage medium for communicating with a mobile device, the computer readable storage medium having computer executable instructions

stored thereon that when installed into a computing device enable the computing device to perform actions, comprising:

receiving a request from the mobile device, wherein the request includes associated information; and

sending at least one device signature to the mobile device based on at least one level of trust determined from a plurality of different levels of trust that is determined, in part, using the associated information, wherein the at lest one level of trust is based on:

if a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device; and

determining if the mobile device is enabled with a defined operational capability and if the mobile device is so enabled, then determining another level of trust associated with the mobile device, and wherein the at least one device signature is determined independent of user authentication.

42. (Currently Amended) The computer readable storage medium of Claim 41, wherein determining the at least one device signature further comprises:

if [[a]]the first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp.

43. (Currently Amended) The computer readable storage medium of Claim 41, wherein determining the at least one device signature further comprises:

if [[a]]the other ~~second~~ level of trust is determined, determining another ~~second~~ tier device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp.

44. (Currently Amended) The computer readable storage medium of Claim 41, wherein determining the at least one device signature further comprises:

if [[a]]the other ~~third~~ level of trust is determined, determining another ~~third~~ tier device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time

45. (Currently Amended) An apparatus for communicating with a mobile device, comprising:

a means for receiving a request from a mobile device, wherein the request includes associated information, wherein the associated information indicates a capability of the mobile device;

a means for automatically determining a plurality of different levels of trust based, in part, on the associated information, wherein at least one of the different levels of trust is based on an operational capability of the mobile device; and

a means for determining a plurality of different device signatures for the mobile device based, in part, on the determined plurality of different levels of trust, and independent of user authentication.